

1 Nathan R. Ring  
2 Nevada State Bar No. 12078  
3 **STRANCH, JENNINGS & GARVEY, PLLC**  
4 3100 W. Charleston Boulevard, Suite 208  
5 Las Vegas, NV 89102  
6 Telephone: (725) 235-9750  
7 [lasvegas@stranchlaw.com](mailto:lasvegas@stranchlaw.com)

8 J. Gerard Stranch IV (*pro hac vice forthcoming*)  
9 **STRANCH, JENNINGS & GARVEY, PLLC**  
10 The Freedom Center  
11 223 Rosa L. Parks Avenue, Suite 200  
12 Nashville, TN 37203  
13 Tel: 615-254-8801  
14 [gstranch@stranchlaw.com](mailto:gstranch@stranchlaw.com)

15 Gary M. Klinger (*pro hac vice forthcoming*)  
16 **MILBERG COLEMAN BRYSON**  
17 **PHILLIPS GROSSMAN, PLLC**  
18 227 W. Monroe Street, Suite 2100  
19 Chicago, IL 60606  
20 Telephone: (866) 252-0878  
21 [gklinger@milberg.com](mailto:gklinger@milberg.com)

22 Ben Barnow (*pro hac vice forthcoming*)  
23 Anthony L. Parkhill (*pro hac vice forthcoming*)  
24 **BARNOW AND ASSOCIATES, P.C.**  
25 205 West Randolph Street, Suite 1630  
26 Chicago, IL 60606  
27 Tel: 312-621-2000  
28 Fax: 312-641-5504  
[b.barnow@barnowlaw.com](mailto:b.barnow@barnowlaw.com)  
[aparkhill@barnowlaw.com](mailto:aparkhill@barnowlaw.com)

*Counsel for Plaintiff and the Proposed Class*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

RATIEK LOWERY, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

NORTHWELL HEALTH, INC. and PERRY  
JOHNSON & ASSOCIATES, INC.,

Defendants.

Case No. 2:23-cv-01857

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Ratiek Lowery (“Plaintiff”), individually, and on behalf of all others similarly situated (collectively, “Class members”), by and through his attorneys, brings this Class Action Complaint against Defendants Northwell Health, Inc. (“Northwell”) and Perry Johnson & Associates, Inc. (“PJA”) (collectively, “Defendants”), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

**INTRODUCTION**

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard his and approximately 3.9 million other individuals’ personally identifying information (“PII”) and personal health information (“PHI”), including names, Social Security numbers, dates of birth, addresses, medical record numbers, encounter numbers, medical information, and dates/times of service.

2. Northwell is the largest health system in New York. PJA is a third-party vendor of health information technology solutions used by Northwell.

3. Between approximately March 27, 2023, and May 2, 2023, an unauthorized third party gained access to PJA’s network system and obtained files containing information about Northwell’s current and former patients (the “Data Breach”).

1           4. Defendants owed a duty to Plaintiff and Class members to implement and maintain  
2 reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against  
3 unauthorized access and disclosure. Defendants breached that duty by, among other things, failing  
4 to implement and maintain reasonable security procedures and practices to protect Northwell's  
5 patients' PII/PHI from unauthorized access and disclosure.  
6

7           5. As a result of Defendants' inadequate security and breach of their duties and  
8 obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and  
9 disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this  
10 action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach,  
11 which occurred between approximately March 27, 2023, and May 2, 2023.  
12

13           6. Plaintiff, on behalf of himself and all other Class members, asserts claims for  
14 negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust  
15 enrichment, and violations of the New York Deceptive Acts and Practices Act, and seeks declaratory  
16 relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief,  
17 and all other relief authorized by law.  
18

## 19 **PARTIES**

### 20 ***Plaintiff Ratiek Lowery***

21           7. Plaintiff Ratiek Lowery is a citizen of New York.

22           8. Plaintiff obtained healthcare or related services from Northwell. As a condition of  
23 receiving services, Northwell required Plaintiff to provide them with his PII/PHI.

24           9. Based on representations made by Northwell, Plaintiff believed Northwell had  
25 implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief  
26 in mind, Plaintiff provided his PII/PHI to Northwell in connection with receiving healthcare services  
27 provided by Northwell.  
28

1           10.     At all relevant times, Defendants stored and maintained Plaintiff's PII/PHI on their  
2 network systems.

3           11.     Plaintiff takes great care to protect his PII/PHI. Had Plaintiff known that Northwell  
4 does not adequately protect the PII/PHI in its possession, including by contracting with companies  
5 that do not adequately protect the PII/PHI in their possession, he would not have obtained healthcare  
6 services from Northwell or agreed to entrust them with his PII/PHI.

7           12.     As a direct result of the Data Breach, Plaintiff has suffered injury and damages  
8 including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the  
9 wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the  
10 value of his PII/PHI; and overpayment for services that did not include adequate data security.

11  
12 ***Defendant Northwell Health, Inc.***

13           13.     Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its  
14 principal place of business at 2000 Marcus Ave., New Hyde Park, NY 11042.

15  
16 ***Defendant Perry Johnson & Associates, Inc.***

17           14.     Defendant Perry Johnson & Associates is a Nevada corporation with its principal  
18 place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. It may be served through its  
19 registered agent C T Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

20  
21 **JURISDICTION AND VENUE**

22           15.     The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. §  
23 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a  
24 citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy  
25 exceeds \$5,000,000, exclusive of interest and costs.

26           16.     This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc.  
27 because it is a corporation incorporated under the laws of Nevada, has its principal place of business  
28 in Nevada, and does significant business in Nevada.

1           17.     This Court has personal jurisdiction over Defendant Northwell Health, Inc., because  
2 it transacts business within this state and makes or performs contracts within this state.

3           18.     Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJA has  
4 its principal place of business in Nevada, and a substantial part of the events giving rise to Plaintiff's  
5 claims arose in this District.  
6

## 7           **FACTUAL ALLEGATIONS**

### 8           ***Overview of Defendants***

9           19.     Northwell is the largest health system in New York.<sup>1</sup> It employs more than 85,000  
10 people at over 900 locations, including 21 hospitals.<sup>2</sup>

11           20.     In the regular course of its business, Northwell collects and maintains the PII/PHI of  
12 its current and former patients. Northwell required Plaintiff and Class members to provide their  
13 PII/PHI as a condition of receiving healthcare services from Northwell.  
14

15           21.     On its website, Northwell claims “patients are our number one priority and we believe  
16 that patient privacy is an integral part of the health care we provide to you.”<sup>3</sup> Northwell states, “To  
17 ensure the development of a lasting bond of trust with our patients, we have many safeguards to  
18 protect the privacy and security of your personal information.”<sup>4</sup> Northwell further promises that  
19 “[w]e also have many policies in place to protect the privacy and security of your personal  
20 information and our employees are educated from the moment they are hired and continually after,  
21 to respect and protect our patient’s privacy.”<sup>5</sup>  
22  
23  
24

---

25           <sup>1</sup> *About Northwell*, NORTHWELL HEALTH, <https://www.northwell.edu/about-northwell> (last accessed Nov. 10, 2023).

26           <sup>2</sup> *Id.*

27           <sup>3</sup> *Patient Privacy Overview*, NORTHWELL HEALTH, <https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy> (last accessed Nov. 10, 2023).

28           <sup>4</sup> *Id.*

<sup>5</sup> *Id.*

22. Northwell’s website contains a Notice of Privacy Practices that “explains how we fulfill our commitment to respect the privacy and confidentiality of your protected health information.”<sup>6</sup> In the Notice, Northwell admits it is “required by law to make sure that information that identifies you is kept private.”

23. The Privacy Policy includes a list of the ways Northwell may use and disclose its patients’ health information, including for treatment, payment, and health care operations, among others.<sup>7</sup> The Privacy Policy promises that disclosures not described in the Notice or permitted by law will be made only with patients’ written authorization.<sup>8</sup>

24. PJA “provides medical transcription services to various healthcare organizations.”<sup>9</sup> Northwell used PJA for medical transcription and dictation services.<sup>10</sup>

25. Plaintiff and Class members are current or former patients of Northwell and entrusted Northwell with their PII/PHI.

### *The Data Breach*

26. Between approximately March 27, 2023, and May 2, 2023, “An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems.”<sup>11</sup>

27. According to the Notice of Data Security Incident posted on PJA’s website, the PII/PHI affected in the Data Breach included names, dates of birth, addresses, medical record

---

<sup>6</sup> *Notice of Privacy Practices*, NORTHWELL HEALTH, <https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf> (last accessed Nov. 10, 2023).

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Cyber Incident Notice*, PERRY JOHNSON & ASSOCS., <https://www.pjats.com/downloads/Notice.pdf> (last accessed Nov. 10, 2023) [hereinafter “*PJA Notice*”].

<sup>10</sup> See Kevin Vesey, *Cyberattack Targets Northwell Health Vendor; Patient Data Compromised*, NEWS12 (Nov. 9, 2023 6:52 PM), <https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach>.

<sup>11</sup> *PJA Notice*, *supra* note 9.

1 numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security  
2 numbers, insurance information, clinical information such as laboratory and diagnostic testing  
3 results, medications, treatment facility names, and healthcare provider names.<sup>12</sup>

4  
5 28. Northwell's Notice of Privacy Practices states, "You have a right to be notified in the  
6 event of a breach of the privacy of your unsecured protected health information by Northwell Health  
7 or its business associates."<sup>13</sup> It promises patients that they "will be notified as soon as reasonably  
8 possible, but no later than 60 days following our discovery of the breach."<sup>14</sup> PJA informed Northwell  
9 of the Data Breach on July 21, 2023,<sup>15</sup> but Northwell failed to notify its patients until early  
10 November, 2023, over three months later.

11 29. Northwell's failure to promptly notify Plaintiff and Class members that their PII/PHI  
12 was accessed and stolen virtually ensured that the unauthorized third parties who exploited those  
13 security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class  
14 members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and  
15 Class members will suffer indefinitely from the substantial and concrete risk that their identities will  
16 be (or already have been) stolen and misappropriated.

17  
18 ***Defendants Knew that Criminals Target PII/PHI***

19 30. At all relevant times, Defendants knew, or should have known, that the information  
20 they collected was a target for malicious actors. Despite such knowledge, Defendants failed to  
21 implement and maintain reasonable and appropriate data privacy and security measures to protect  
22 Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated  
23 and guarded against.  
24

25  
26  
27 <sup>12</sup> *Id.*

28 <sup>13</sup> *Notice of Privacy Practices, supra* note 6.

<sup>14</sup> *Id.*

<sup>15</sup> *Vesey, supra* note 10.

1           31. It is well known among companies that store sensitive personally identifying  
2 information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and  
3 frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches are  
4 on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws  
5 in . . . systems either online or in stores.”<sup>16</sup>

6  
7           32. Cyber criminals seek out PHI at a greater rate than other sources of personal  
8 information. In a 2023 report, the healthcare compliance company Protenus found that there were  
9 956 medical data breaches in 2022 with over 59 million patient records exposed.<sup>17</sup> This is an increase  
10 from the 758 medical data breaches which exposed approximately 40 million records that Protenus  
11 compiled in 2020.<sup>18</sup>

12  
13           33. PII/PHI is a valuable property right.<sup>19</sup> The value of PII/PHI as a commodity is  
14 measurable.<sup>20</sup> “Firms are now able to attain significant market valuations by employing business  
15 models predicated on the successful use of personal data within the existing legal and regulatory  
16 frameworks.”<sup>21</sup> American companies are estimated to have spent over \$19 billion on acquiring

17  
18  
19  
20  
21           <sup>16</sup> Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently,*  
22 *your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.),  
<https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

23           <sup>17</sup> See 2023 *Breach Barometer*, PROTENUS, <https://www.protenus.com/breach-barometer-report> (last  
24 accessed Nov. 10, 2023).

25           <sup>18</sup> See *id.*

26           <sup>19</sup> See Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information  
27 Processing 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to  
28 collect as much data about personal conducts and preferences as possible...”),  
[https://www.researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data).

29           <sup>20</sup> See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*,  
MEDSCAPE.COM (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

30           <sup>21</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary*  
31 *Value*, OECD ILIBRARY (April 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)  
32 [the-economics-of-personal-data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en).

1 personal data of consumers in 2018.<sup>22</sup> It is so valuable to identity thieves that once PII has been  
 2 disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

3 34. As a result of the real and significant value of these data, identity thieves and other  
 4 cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive  
 5 information directly on various internet websites making the information publicly available. This  
 6 information from various breaches, including the information exposed in the Data Breach, can be  
 7 readily aggregated with other such data and become more valuable to thieves and more damaging to  
 8 victims.  
 9

10 35. PHI is particularly valuable and has been referred to as a “treasure trove for  
 11 criminals.”<sup>23</sup> A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten  
 12 personal identifying characteristics of an individual.”<sup>24</sup>  
 13

14 36. All-inclusive health insurance dossiers containing sensitive health insurance  
 15 information, names, addresses, telephone numbers, email addresses, SSNs, and bank account  
 16 information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on  
 17 the black market.<sup>25</sup> According to a report released by the Federal Bureau of Investigation’s (“FBI”)  
 18 Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security  
 19 or credit card number.<sup>26</sup>  
 20

21  
 22 <sup>22</sup> IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018),  
 23 <https://www.iab.com/news/2018-state-of-data-report/>.

24 <sup>23</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019),  
 25 <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

26 <sup>24</sup> *Id.*

27 <sup>25</sup> See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

28 <sup>26</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illuminweb.com/wp-content/uploads/illmo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

37. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”<sup>27</sup> Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”<sup>28</sup>

38. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”<sup>29</sup>

39. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

### ***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

40. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.<sup>30 31</sup>

<sup>27</sup> Steager, *supra* note 23.

<sup>28</sup> *Id.*

<sup>29</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

<sup>30</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM’N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed Nov. 10, 2023).

<sup>31</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 12 C.F.R. § 1022.3(h). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 12 C.F.R. § 1022.3(g).

41. Experian, one of the largest credit reporting companies in the world, warns consumers that “[i]dentity thieves can profit off your personal information” by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.<sup>32</sup>

42. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.<sup>33</sup>

43. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”<sup>34</sup> It “is also more difficult to detect, taking almost twice as long as normal identity theft.”<sup>35</sup> In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”<sup>36</sup> The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to use.”<sup>37</sup>

44. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing

<sup>32</sup> See Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

<sup>33</sup> Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), <https://www.idtheftcenter.org/publication/2023-consumer-impact-report/> (last accessed Nov. 10, 2023).

<sup>34</sup> Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), [http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF\\_Geography\\_of\\_Medical\\_Identity\\_Theft\\_fs.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).

<sup>35</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 26.

<sup>36</sup> See *What to Know About Medical Identity Theft*, FED. TRADE COMM’N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Nov. 10, 2023).

<sup>37</sup> *Id.*

1 harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already  
 2 been suffered by the victim.

3 45. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other  
 4 PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent  
 5 activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find  
 6 flaws in their computer systems, as stating, “If I have your name and your Social Security number  
 7 and you don’t have a credit freeze yet, you’re easy pickings.”<sup>38</sup>

9 46. A report published by the World Privacy Forum and presented at the US FTC  
 10 Workshop on Informational Injury describes what medical identity theft victims may experience:

- 11 a. Changes to their health care records, most often the addition of falsified  
 12 information, through improper billing activity or activity by imposters. These  
 13 changes can affect the healthcare a person receives if the errors are not caught  
 14 and corrected.
- 15 b. Significant bills for medical goods and services neither sought nor received.
- 16 c. Issues with insurance, co-pays, and insurance caps.
- 17 d. Long-term credit problems based on problems with debt collectors reporting  
 18 debt due to identity theft.
- 19 e. Serious life consequences resulting from the crime; for example, victims have  
 20 been falsely accused of being drug users based on falsified entries to their  
 21 medical files; victims have had their children removed from them due to  
 22 medical activities of the imposter; victims have been denied jobs due to  
 23 incorrect information placed in their health files due to the crime.
- 24 f. As a result of improper and/or fraudulent medical debt reporting, victims may  
 25 not qualify for mortgage or other loans and may experience other financial  
 26 impacts.
- 27 g. Phantom medical debt collection based on medical billing or other identity  
 28 information.

---

<sup>38</sup> Patrick Lucas Austin, *‘It Is Absurd.’ Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.<sup>39</sup>

47. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.<sup>40</sup>

### ***Damages Sustained by Plaintiff and Class Members***

48. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

### **CLASS ALLEGATIONS**

49. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

50. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

All United States residents whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

<sup>39</sup> See Dixon & Emerson, *supra* note 34.

<sup>40</sup> John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

1  
2 51. Excluded from the Class are Northwell Health, Inc., and its affiliates, parents,  
3 subsidiaries, employees, officers, agents, and directors; Perry Johnson & Associates, Inc., and its  
4 affiliates, parents, subsidiaries, employees, officers, agents, and directors; as well as the judge(s)  
5 presiding over this matter and the clerks of said judge.

6 52. Certification of Plaintiff's claims for class-wide treatment is appropriate because  
7 Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would  
8 be used to prove those elements in individual actions alleging the same claims.  
9

10 53. The members in the Class are so numerous that joinder of each of the Class members  
11 in a single proceeding would be impracticable. Northwell initially indicated that approximately 3.9  
12 million patients were affected by the Data Breach.<sup>41</sup>

13 54. Common questions of law and fact exist as to all Class members and predominate over  
14 any potential questions affecting only individual Class members. Such common questions of law or  
15 fact include, *inter alia*:

- 16 a. Whether Defendants had a duty to implement and maintain reasonable
- 17 security procedures and practices to protect and secure Plaintiff's and
- 18 Class members' PII/PHI from unauthorized access and disclosure;
- 19 b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and
- 20 Class members to unauthorized third parties;
- 21 c. Whether Defendants failed to exercise reasonable care to secure and
- 22 safeguard Plaintiff's and Class members' PII/PHI;
- 23 d. Whether an implied contract existed between Class members and
- 24 Defendants, providing that Defendants would implement and maintain
- 25 reasonable security measures to protect and secure Class members'
- 26 PII/PHI from unauthorized access and disclosure;
- 27 e. Whether Defendants engaged in unfair, unlawful, or deceptive practices
- 28 by failing to safeguard the PII/PHI of Plaintiff and Class members;

---

<sup>41</sup> See Vesey, *supra* note 10.

- 1 f. Whether Defendants breached their duties to protect Plaintiff's and Class  
2 members' PII/PHI; and
- 3 g. Whether Plaintiff and Class members are entitled to damages and the  
4 measure of such damages and relief.

5 55. Defendants engaged in a common course of conduct giving rise to the legal rights  
6 sought to be enforced by Plaintiff, on behalf of himself and all other Class members. Individual  
7 questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions  
8 that dominate this action.

9 56. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed  
10 members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members  
11 were injured by the same wrongful acts, practices, and omissions committed by Defendants, as  
12 described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that  
13 give rise to the claims of all Class members.

14 57. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff  
15 is an adequate representative of the Class in that he has no interests adverse to, or that conflict  
16 with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and  
17 success in the prosecution of complex consumer protection class actions of this nature.

18 58. A class action is superior to any other available means for the fair and efficient  
19 adjudication of this controversy, and no unusual difficulties are likely to be encountered in the  
20 management of this class action. The damages and other financial detriment suffered by Plaintiff  
21 and Class members are relatively small compared to the burden and expense that would be required  
22 to individually litigate their claims against Defendants, so it would be impracticable for Class  
23 members to individually seek redress from Defendants' wrongful conduct. Even if Class members  
24 could afford individual litigation, the court system could not. Individualized litigation creates a  
25 potential for inconsistent or contradictory judgments, and increases the delay and expense to all  
26 parties and the court system. By contrast, the class action device presents far fewer management  
27  
28

difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CAUSES OF ACTION**

### **COUNT I** **NEGLIGENCE**

59. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

60. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

61. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare providers that collect and store PII/PHI in recent years.

62. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

63. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

64. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or

1 contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage,  
2 monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and  
3 software and hardware systems would result in the unauthorized release, disclosure, and  
4 dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

5  
6 65. But for Defendants' negligent conduct or breach of the above-described duties owed  
7 to Plaintiff and Class members, their PII/PHI would not have been compromised.

8 66. As a result of Defendants' above-described wrongful actions, inaction, and want of  
9 ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members  
10 have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in  
11 the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii)  
12 out-of-pocket expenses associated with the prevention, detection, and recovery from  
13 unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting  
14 to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their  
15 PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and  
16 money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised  
17 as a result of the Data Breach; and (vii) overpayment for the services that were received without  
18 adequate data security.  
19  
20

21 **COUNT II**  
22 **NEGLIGENCE PER SE**

23 67. Plaintiff realleges and incorporates by reference all preceding paragraphs as if  
24 fully set forth herein.

25 68. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for  
26 Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts  
27 A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic  
28

1 Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively,  
2 “HIPAA Privacy and Security Rules”).

3 69. Defendants’ duties also arise from Section 5 of the FTC Act (“FTCA”), 15 U.S.C.  
4 § 45(a)(1), which prohibits “unfair . . . practices in or affecting commerce,” including, as  
5 interpreted by the FTC, the unfair act or practice by business, such as Northwell, of failing to  
6 employ reasonable measures to protect and secure PII/PHI.

7  
8 70. Defendants violated HIPAA Privacy and Security Rules, Section 5 of the FTCA,  
9 and IPIPA by failing to, or contracting with companies that failed to, use reasonable measures  
10 to protect Plaintiff’s and other Class members’ PII/PHI, by failing to provide timely notice, and  
11 by not complying with applicable industry standards. Defendants’ conduct was particularly  
12 unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable  
13 consequences of a data breach involving PII/PHI including, specifically, the substantial  
14 damages that would result to Plaintiff and the other Class members.

15  
16 71. Defendants’ violation of the HIPAA Privacy and Security Rules and Section 5 of  
17 the FTCA constitutes negligence per se.

18 72. Plaintiff and Class members are within the class of persons that the HIPAA  
19 Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

20  
21 73. The harm occurring as a result of the Data Breach is the type of harm that the  
22 HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.  
23 The FTC has pursued enforcement actions against businesses, which, as a result of their failure  
24 to employ reasonable data security measures and avoid unfair practices or deceptive practices,  
25 caused the same type of harm that has been suffered by Plaintiff and Class members as a result  
26 of the Data Brach.

27 74. It was reasonably foreseeable to Defendants that their failure to exercise reasonable  
28 care in safeguarding and protecting Plaintiff’s and Class members’ PII/PHI by failing to, or

1 contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage,  
2 monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and  
3 software and hardware systems, would result in the release, disclosure, and dissemination of  
4 Plaintiff's and Class members' PII/PHI to unauthorized individuals.

5  
6 75. The injury and harm that Plaintiff and the other Class members suffered was the direct  
7 and proximate result of Defendants' violations of harm the HIPAA Privacy and Security Rules and  
8 Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury,  
9 including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the  
10 compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the  
11 prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity  
12 costs associated with effort attempting to mitigate the actual and future consequences of the Data  
13 Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future  
14 costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact  
15 of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services  
16 that were received without adequate data security.

17  
18 **COUNT III**  
19 **BREACH OF FIDUCIARY DUTY**  
20 ***Against Northwell Only***

21 76. Plaintiff reallege and incorporate by reference all preceding paragraphs as if fully  
22 set forth herein.

23 77. This claim is brought by Plaintiff on behalf of all Class members who provided  
24 their PII/PHI to Northwell.

25 78. Plaintiff and Class members gave Northwell their PII/PHI in confidence,  
26 believing that Northwell would protect that information. Plaintiff and Class members would not  
27 have provided Northwell with this information had they known it would not be adequately  
28 protected. Northwell's acceptance and storage of Plaintiff's and Class members' PII/PHI created

1 a fiduciary relationship between Northwell and Plaintiff and Class members. In light of this  
2 relationship, Northwell must act primarily for the benefit of its patients, which includes  
3 safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

4  
5 79. Due to the nature of the relationship between Northwell and Plaintiff and Class  
6 members, Plaintiff and Class members were entirely reliant upon Northwell to ensure that their  
7 PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or  
8 influencing the nature and extent of Northwell's or its vendors data security policies and  
9 practices, and Northwell was in an exclusive position to guard against the Data Breach.

10  
11 80. Northwell has a fiduciary duty to act for the benefit of Plaintiff and Class  
12 Members upon matters within the scope of their relationship. They breached that duty by  
13 contracting with companies that failed to, properly protect the integrity of the system containing  
14 Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set  
15 forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that  
16 they collected.

17  
18 81. As a direct and proximate result of Northwell's breaches of its fiduciary duties,  
19 Plaintiff and Class members have suffered and will suffer injury, including, but not limited to:  
20 (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft  
21 of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery  
22 from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting  
23 to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their  
24 PII/PHI which remains in Northwell's possession; (vi) future costs in terms of time, effort, and  
25 money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as  
26 a result of the Data Breach; and (vii) overpayment for the services that were received without  
27 adequate data security.  
28

#### **COUNT IV**

**BREACH OF IMPLIED CONTRACT**  
***Against Northwell Only***

82. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

83. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to Northwell.

84. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Northwell.

85. Pursuant to these implied contracts, Plaintiff and Class members paid money to Northwell, directly or through their insurance, and provided Northwell with their PII/PHI. In exchange, Northwell agreed to, among other things, and Plaintiff and Class members understood that Northwell would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

86. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Northwell, on the other hand. Indeed, as set forth *supra*, Northwell recognized the importance of data security and the privacy of Northwell's patients' PII/PHI. Had Plaintiff and Class members known that Northwell would not adequately protect their PII/PHI, they would not have received healthcare or other services from Northwell.

87. Plaintiff and Class members performed their obligations under the implied contract when they provided Northwell with their PII/PHI and paid for healthcare or other services from Northwell.

88. Northwell breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect

1 and secure their PII/PHI, including by ensuring companies it contracts with implement and  
2 maintain reasonable security measures to protect PII/PHI, and in failing to implement and  
3 maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in  
4 a manner that complies with applicable laws, regulations, and industry standards.

5  
6 89. Northwell's breach of its obligations of its implied contracts with Plaintiff and  
7 Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other  
8 Class members have suffered from the Data Breach.

9  
10 90. Plaintiff and all other Class members were damaged by Northwell's breach of  
11 implied contracts because: (i) they paid—directly or through their insurers—for data security  
12 protection they did not receive; (ii) they face a substantially increased risk of identity theft and  
13 medical theft—risks justifying expenditures for protective and remedial services for which they are  
14 entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals;  
15 (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of  
16 their PII/PHI, for which there is a well-established national and international market; (vi) lost time  
17 and money incurred to mitigate and remediate the effects of the Data Breach, including the increased  
18 risks of identity theft they face and will continue to face; and (vii) overpayment for services that  
19 were received without adequate data security.

20  
21 **COUNT V**  
22 **UNJUST ENRICHMENT**

23 91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if  
24 fully set forth herein.

25 92. This claim is pleaded in the alternative to the breach of implied contract claim.

26 93. Plaintiff and Class members conferred a monetary benefit upon Defendants in the  
27 form of monies paid to Northwell for healthcare services, which Northwell used in turn to pay for  
28 PJA's services, and through the provision of their PII/PHI.

1 94. Defendants accepted or had knowledge of the benefits conferred upon them by  
 2 Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class  
 3 members' PII/PHI, as this was used to facilitate billing services and services provided to Northwell.

4 95. As a result of Defendants' conduct, Plaintiff and Class members suffered actual  
 5 damages in an amount equal to the difference in value between their payments made with reasonable  
 6 data privacy and security practices and procedures that Plaintiff and Class members paid for, and  
 7 those payments without reasonable data privacy and security practices and procedures that they  
 8 received.  
 9

10 96. Defendants should not be permitted to retain the money belonging to Plaintiff and  
 11 Class members because Defendants failed to adequately implement the data privacy and security  
 12 procedures for themselves that Plaintiff and Class members paid for and that were otherwise  
 13 mandated by federal, state, and local laws and industry standards.  
 14

15 97. Plaintiff and Class members have no adequate remedy at law.

16 98. Defendants should be compelled to provide for the benefit of Plaintiff and Class  
 17 members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged  
 18 herein.  
 19

20 **COUNT VI**  
**VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT,**  
**N.Y. Gen. Bus. Law § 349 ("GBL")**  
***Against Northwell Only***

21 99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if  
 22 fully set forth herein.  
 23

24 100. New York General Business Law § 349(a) states, "Deceptive acts or practices in the  
 25 conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby  
 26 declared unlawful."  
 27  
 28

1           101. Northwell is a “person, firm, corporation or association or agent or employee thereof”  
2 within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b). At all relevant times, Northwell was  
3 engaged in “business,” “trade,” or “commerce” within the meaning of the GBL. *See* N.Y. Gen. Bus.  
4 Law § 349(a).

5           102. Plaintiff and Class members are “persons” within the meaning of Gen. Bus. Law  
6 § 349(h).

7           103. Northwell promised to protect, but subsequently failed to adequately safeguard and  
8 maintain, Plaintiff’s and Class members’ PII/PHI. Northwell failed to notify Plaintiff and other Class  
9 members that, contrary to its representations about valuing data security and privacy, it does not  
10 maintain adequate controls to protect their PII/PHI, including by ensuring companies it contracts  
11 with maintain adequate data protection practices.

12           104. Had Plaintiff and Class members been aware that Northwell omitted or  
13 misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and Class  
14 members would not have accepted services from Northwell.

15           105. Northwell’s failure to make Plaintiff and Class members aware that it would not  
16 adequately safeguard their information, while maintaining that it would, is a “deceptive act or  
17 practice” under N.Y. Gen. Bus. Law § 349.

18           106. Plaintiff and all other Class members were damaged by Northwell’s unfair and  
19 deceptive trade practices because: (i) they paid—directly or through their insurers—for data  
20 security protection they did not receive; (ii) they face a substantially increased risk of identity theft  
21 and medical theft—risks justifying expenditures for protective and remedial services for which they  
22 are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized  
23 individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the  
24 value of their PII/PHI, for which there is a well-established national and international market; (vi)  
25 lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the  
26  
27  
28

1 increased risks of identity theft they face and will continue to face; and (vii) overpayment for services  
2 that were received without adequate data security.

3 107. Pursuant to Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of himself  
4 and Class members in the amount of the greater of actual damages or \$50 for each violation of  
5 N.Y. Gen. Bus. Law § 349. Because Northwell's conduct was committed willfully and  
6 knowingly, Plaintiff and Class members are entitled to recover up to three times their actual  
7 damages, up to \$1,000.  
8

9 **PRAYER FOR RELIEF**

10 Plaintiff, individually and on behalf of all other members of the Class, respectfully  
11 requests that the Court enter judgment in his favor and against Defendants as follows:  
12

13 A. Certifying the Class as requested herein, designating Plaintiff as Class  
14 Representative, and appointing Plaintiff's counsel as Class Counsel;

15 B. Awarding Plaintiff and the Class appropriate monetary relief, including actual  
16 damages, statutory damages, punitive damages, restitution, and disgorgement;

17 C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as  
18 may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive  
19 relief designed to prevent Defendants from experiencing another data breach by adopting and  
20 implementing best data security practices to safeguard PII/PHI and to provide or extend credit  
21 monitoring services and similar services to protect against all types of identity theft and medical  
22 identity theft;  
23

24 D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the  
25 maximum extent allowable;

26 E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses,  
27 as allowable; and  
28

1 F. Awarding Plaintiff and the Class such other favorable relief as allowable under  
2 law.

3 **JURY TRIAL DEMANDED**

4 Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.  
5

6 Dated: November 13, 2023

Respectfully submitted,

7 /s/ Nathan R. Ring

8 Nathan R. Ring

9 Nevada State Bar No. 12078

10 **STRANCH, JENNINGS & GARVEY, PLLC**

3100 W. Charleston Boulevard, Suite 208

Las Vegas, NV 89102

Tel: 725-235-9750

nring@stranchlaw.com

13 J. Gerard Stranch IV\*

**STRANCH, JENNINGS & GARVEY, PLLC**

The Freedom Center

223 Rosa L. Parks Avenue, Suite 200

Nashville, TN 37203

Tel: 615-254-8801

gstranch@stranchlaw.com

17 Gary M. Klinger\*

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, PLLC**

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Telephone: (866) 252-0878

[gklinger@milberg.com](mailto:gklinger@milberg.com)

22 Ben Barnow\*

Anthony L. Parkhill\*

**BARNOW AND ASSOCIATES, P.C.**

205 West Randolph Street, Suite 1630

Chicago, IL 60606

Tel: 312-621-2000

Fax: 312-641-5504

b.barnow@barnowlaw.com

aparkhill@barnowlaw.com

*Attorneys for Plaintiff and the Proposed Class*

*\*pro hac vice forthcoming*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102

**SJC** 725-235-9750  
lasvegas@stranchlaw.com

STRANCH, JENNINGS & GARVEY  
PLLC